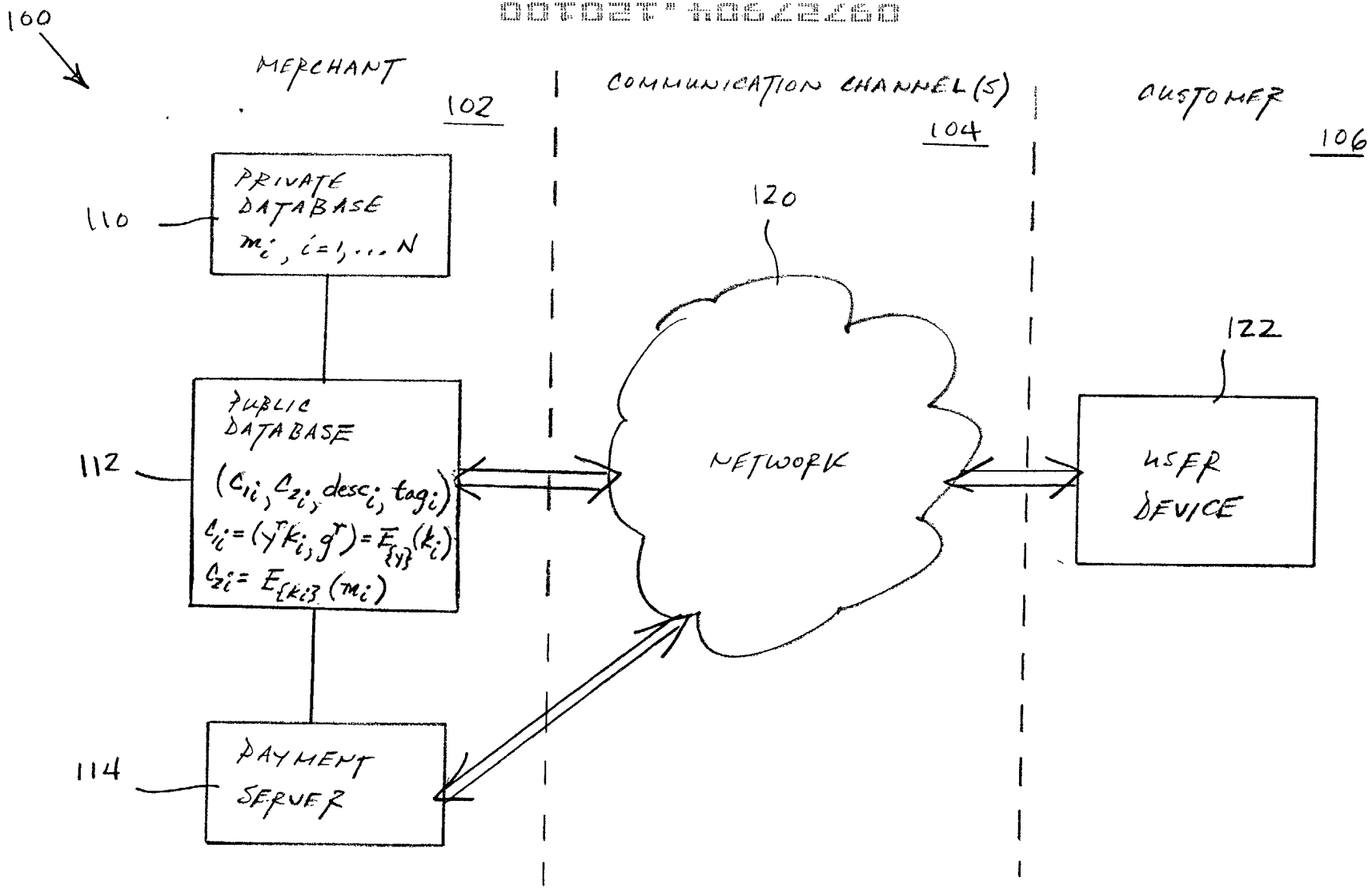
100
MERCHANT
102
COMMUNICATION CHANNEL(S)
104
CUSTOMER
106
110
PRIVATE DATABASE
m_i, $i=1,\ldots N$
120
122
112
PUBLIC DATABASE
$(C_{1i}, C_{2i}, desc_i, tag_i)$
$C_{1i} = (Y^r k_i, g^r) = E_{\{y\}}(k_i)$
$C_{2i} = E_{\{ki\}}(m_i)$
NETWORK
USER DEVICE
114
PAYMENT SERVER

FIG. 1

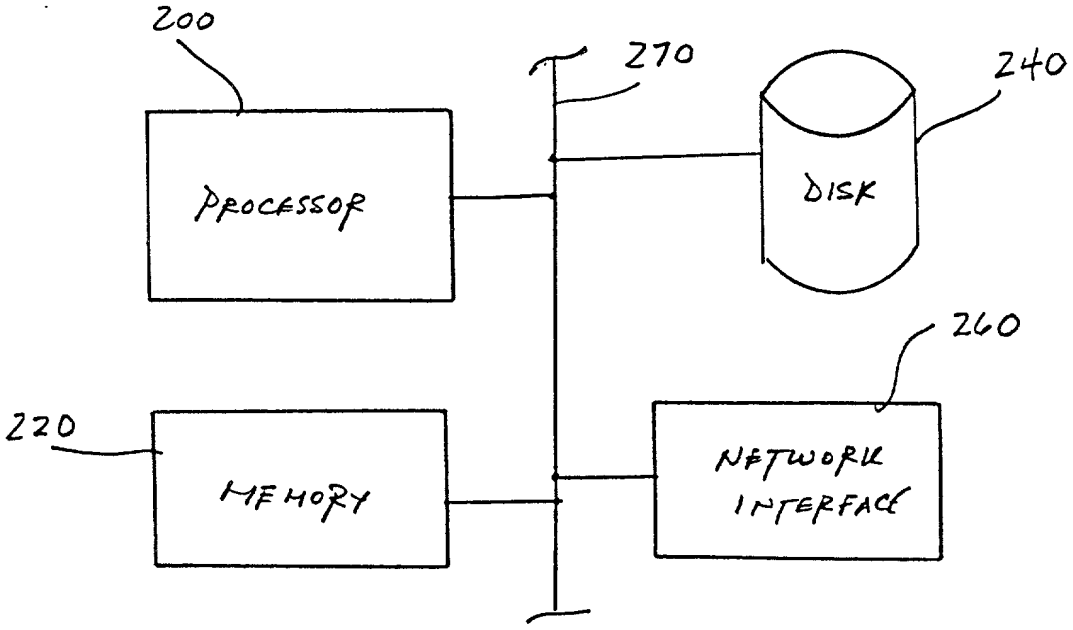
200
270
240
PROCESSOR
DISK
260
220
MEMORY
NETWORK
INTERFACE

FIG. 2

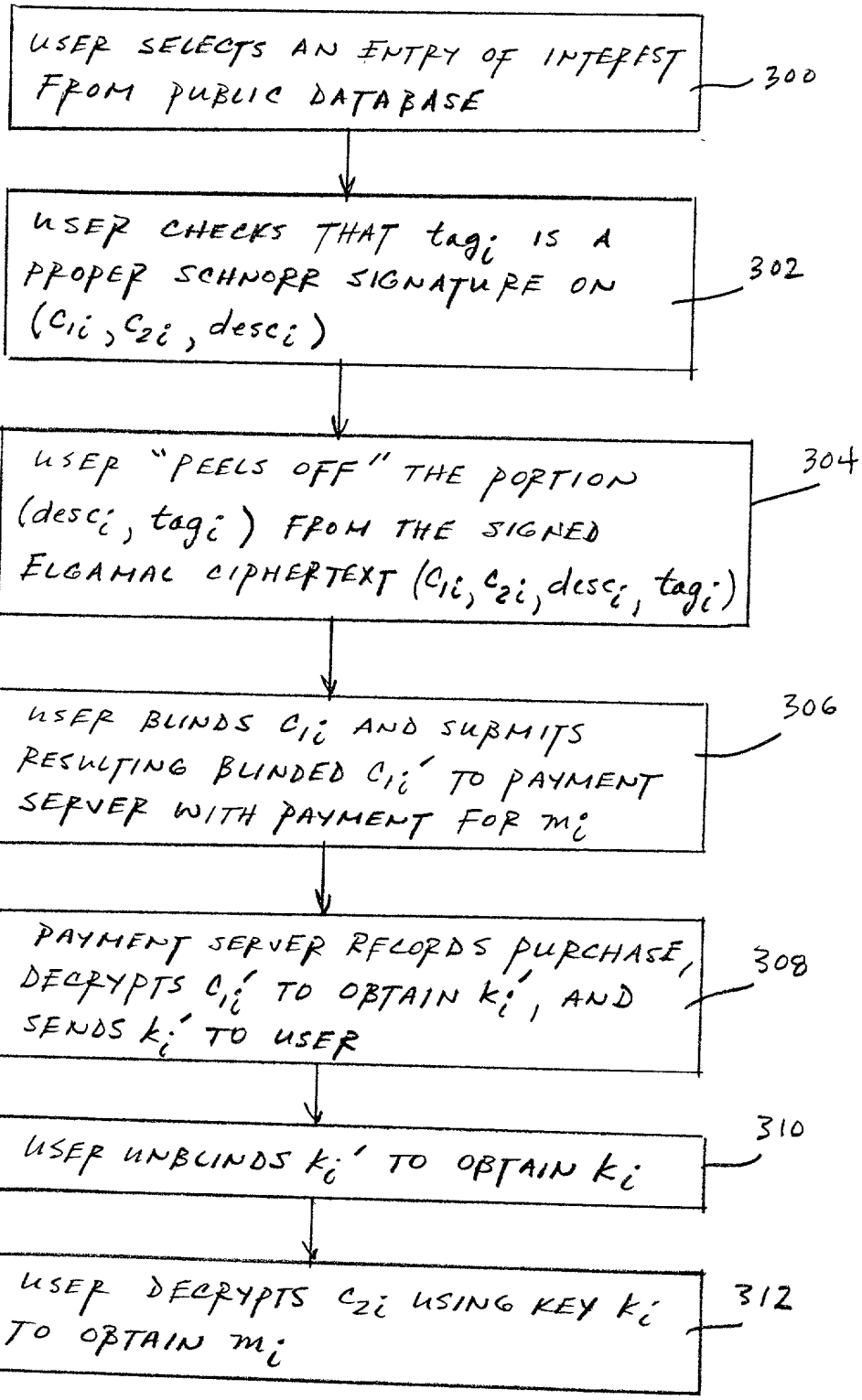
USER SELECTS AN ENTRY OF INTEREST FROM PUBLIC DATABASE
300
USER CHECKS THAT tag_i IS A PROPER SCHNORR SIGNATURE ON $(c_{1i}, c_{2i}, desc_i)$
302
USER "PEELS OFF" THE PORTION $(desc_i, tag_i)$ FROM THE SIGNED ELGAMAL CIPHERTEXT $(c_{1i}, c_{2i}, desc_i, tag_i)$
304
USER BLINDS c_{1i} AND SUBMITS RESULTING BLINDED c_{1i}' TO PAYMENT SERVER WITH PAYMENT FOR m_i
306
PAYMENT SERVER RECORDS PURCHASE, DECRYPTS c_{1i}' TO OBTAIN k_i', AND SENDS k_i' TO USER
308
USER UNBLINDS k_i' TO OBTAIN k_i
310
USER DECRYPTS c_{2i} USING KEY k_i TO OBTAIN m_i
312

FIG. 3